UNITED STATES PATENT APPLICATION FOR

<u>METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER</u>

Inventor:

Ryuichi Iwamura

Prepared by:

WAGNER, MURABITO & HAO LLP

TWO NORTH MARKET STREET

THIRD FLOOR

SAN JOSE, CALIFORNIA 95113

(408) 938-9060

METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER

FIELD OF THE INVENTION

The present invention relates to the field of digital signal processing.

5   Specifically, the present invention relates to a system and method for securely

decoding an encrypted digital signal.

BACKGROUND ART

The field of digital video signal processing has seen rapid development in

10   recent years. For example, digital broadcasting is now beginning to replace

analog broadcasting. Digital broadcasting must be securely protected, as digital

broadcast data can easily be copied without degrading the quality of the content.

Currently, most digital broadcast streams are encrypted, for example, with Data

Encryption Standard (DES). When using DES, the broadcast service provider

15   provides a Smartcard to each subscriber. The Smartcard is inserted in a set-top

box, which communicates with the Smartcard to generate an encryption key. The

key is sent to a decryptor, which decrypts the encrypted stream with the key. The

key is renewed frequently, for example every five seconds.

20   A conventional digital cable set-top box 130 for decrypting and decoding a

digital signal is illustrated in Figure 1. When playing a signal which is currently

being received, front-end 150 tunes to a digital cable signal, demodulates and

sends the signal to broadcast decryptor 152. The bitstream decrypted by

broadcast decryptor 152 is sent to transport parser/de-multiplexer 162 through

25   switch 155. In this mode, switch 155 connects broadcast decryptor 152 in chip A

180 to transport parser/de-multiplexer 162 in chip B 190. Thus, unfortunately, the decrypted signal is exposed ("in the clear") on a pin of chip A 180 and chip B 190. Therefore, in this conventional system, the decrypted bitstream is vulnerable to being stolen, copied, and distributed without the copyright-holder's consent.

5

After chip B 190 receives the signal, transport parser/de-multiplexer 162 parses and de-multiplexes the decrypted bitstream. Then, it sends video packets to video decoder 170 and audio decoder 172, respectively. Video decoder 170 decodes the video data and sends the decoded signal to a television set 174. Similarly, audio decoder 172 decodes the audio data and sends the decoded

10 signal to television set 174.

Chip A 180 contains necessary circuitry for protecting the signal when it is transported for storage. In the recording mode, the decrypted bitstream from broadcast decryptor 152 is re-encrypted in Digital Transmission Content

15 Protection (DTCP) block 154. DTCP is the encryption for the IEEE 1394 serial bus. The re-encrypted bitstream is sent to hard disk drive (HDD) 158 via the IEEE 1394 bus 176.

When playing back the recorded signal, the bitstream is transferred from

20 HDD 158 though the IEEE 1394 interface 156 to the DTCP block 154, where the signal is decrypted. The decrypted signal is sent to transport parser/de-multiplexer 162 and decoded as described above. Thus, while the signal is encrypted while on the IEEE 1394 bus, unfortunately, it is not encrypted (e.g., it is in the clear) while

being transferred between chip A 180 and chip B 190. Again, the un-encrypted bitstream is vulnerable to theft when it is transferred between the two chips.

5 The received bitstream contains encryption information. Transport parser/de-multiplexer 162 extracts encryption key data from the decrypted bitstream and sends it to the host CPU 114 though bus interface 164 via PCI bus 115. The host CPU 114 communicates with the Smartcard 113 through Smartcard interface 110 to generate the encryption keys. The Smartcard 113 is a 'black box,' for example, the internal signal process is kept secret.

10

The host CPU 114 sends the keys to the broadcast decryptor 152 over the PCI bus 115. The broadcast decryptor 152, in turn, uses the keys to decrypt the incoming stream. Because the keys are frequently renewed, the host CPU 114 must generate and send a new key to the broadcast decryptor 152 within the time
15 period specified in the requirements. When an even key is currently being used by the broadcast decryptor 152, a new odd key is sent to broadcast decryptor 152. The broadcast decryptor 152 has an even and an odd key register.

The received bitstream also contains encryption information that is used by
20 the decryptor directly. For example, the Motion Pictures Expert Group 2 (MPEG-2) packet header contains transport scrambling control (TSC) bits. The TSC bits tell whether the packet is encrypted and whether the encryption key was even or odd. Based on the TSC bits, the broadcast decryptor 152 selects either the even or the odd key to decrypt the packet. After decryption, the TSC bits in the header are
25 reset to 'un-encrypted.'

SONY-50P4042 US P

Unfortunately, this conventional system exposes the encryption key on the PCI bus 115 when the CPU 114 transfers the key to the decryptor 152. Consequently, it is possible to steal the key by monitoring the PCI bus 115. If a

5   series of keys are stolen, it is possible to determine the actual key generation mechanism. Once the key generation mechanism is known, access to programs for which a fee is charged is no longer secure. Even if the key generation mechanism is not determined, the stolen keys can be sent over a network to other set-top boxes, thus defeating the encryption.

SUMMARY OF THE INVENTION

Therefore, it would be advantageous to provide a method and system providing for a secure digital signal decryptor and decoder. A further need exists for a method and/or system which decrypts and decodes a signal without exposing

5   a decrypted signal on the pins of a integrated circuit when the signal is transferred between two integrated circuits. A still further need exists for such a system which does not expose an encryption key on a communication link.

The present invention provides a method and system providing for a secure

10   digital signal decryptor. Embodiments provides a method and system which decrypt and decode a signal without exposing the decrypted signal on the pins of an integrated circuit. Embodiments provide a method and system which decrypt and decode a signal without exposing an encryption key on a communication bus. The present invention provides these advantages and others not specifically

15   mentioned above but described in the sections to follow.

A method and system for securely decrypting and decoding a digital signal is disclosed. One embodiment of the present invention first receives an encrypted signal at a first logical circuit. Next, this embodiment determines a broadcast

20   encryption key for the encrypted signal at a first location separate from the first logical circuit. For example, the separate location where the broadcast key was determined may be across a communication link from the first circuit where the signal is being received. Then, the broadcast encryption key is encrypted and transferred over the communication link. Next, at the first logical circuit, the

25   encrypted broadcast encryption key is decrypted. Therefore, the broadcast

encryption key is determined. Then, at said first logical circuit, the encrypted

signal is decrypted using the broadcast encryption key. Consequently, the

encrypted signal is decrypted without exposing the broadcast encryption key on

the communication link in an un-encrypted form, for example, without exposing the

5   un-encrypted signal in the clear.

Another embodiment of the present invention, in addition to the steps in the

above paragraph, accesses a value in a hidden register on the first logical circuit.

Using this value, the broadcast encryption key is encrypted. The first circuit may

10   then use the value in its hidden register to decrypt the broadcast key when it

receives it. In still another embodiment, the hidden register may be written to.

In yet another embodiment, a value is stored in a hidden register on the first

logical circuit, for example, at manufacture time. This value is provided to a host

15   computer system, which uses the value for encryption purposes.

In another embodiment, at least one of a plurality of hidden registers on the

first logical circuit is selected to be used to encrypt the broadcast encryption key.

Then, the selected register(s) are indicated to the first logical circuit.

20

In one embodiment, a value in non-volatile memory on the first logical

circuit is accessed. Using this value, an encryption key is encrypted. In one

embodiment, the non-volatile memory contains user-dependent data.

Yet another embodiment provides a method which first generates a local encryption key. Then, the local encryption key is transferred across a communication link to a first logical circuit and to a second logical circuit. With the local encryption key, a digital signal at the first logical circuit is encrypted. This

5 encrypted signal is transferred to the second logical circuit. Thus, the signal is not exposed in an un-encrypted form. Next, the second logical circuit uses the local encryption key to decrypt the signal.

In another embodiment, the host processor accesses a value in a register

10 on the first circuit, which it uses to encrypt the local encryption key before it is transferred across the communication link to the first circuit. In a similar fashion, the host process access a register on the second circuit, which is used to encrypt the local key before it is sent to the second circuit. The first and second circuits use the values in their respective hidden registers to decrypt the local keys.

15

In yet another embodiment, in addition to the steps in the above paragraph, a command is issued to the first logical circuit to modify a header in the signal bitstream to indicate that the bitstream is encrypted. Furthermore, the command may indicate the type of encryption key, for example, odd or even.

20

A still another embodiment provides for a system for processing a digital signal. The system comprises a first logical circuit comprising a first hidden register and a local encryptor. The first logical circuit is operable to decrypt a first local key using a first value stored in the first register. The system also comprises

25 a second logical circuit which, in turn, comprises a local decryptor and a second

hidden register. The second logical circuit is operable to decrypt a second local key using a second value stored in the second register. Furthermore, the local decryptor is operable to decrypt a signal encrypted with the local encryptor. Thus, the system is able to decrypt the received broadcast signal without exposing an

5   un-encrypted encryption key and without exposing an un-encrypted broadcast signal.

Another embodiment adds a host processor and memory to this system. A communication link connects the host processor to the first logical circuit and to the

10   second logical circuit. The memory contains instructions, which when run on the host processor, are operable to access the first hidden register and generate the first local key and to access the second hidden register and generate the second local key.

15   In still another embodiment, the first logical circuit further comprises a plurality of hidden registers and a control register operable to store a value to indicate which of the hidden registers is used for encryption purposes.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration of a conventional digital bitstream decryptor and decoder.

5   Figure 2 is an illustration of an exemplary digital bitstream decryptor and decoder, according to an embodiment of the present invention.

Figure 3a is an illustration of a local encryptor, according to an embodiment of the present invention.

10

Figure 3b is an illustration of a local decryptor, according to an embodiment of the present invention.

Figure 4 is a flowchart illustrated the steps of a process of securely

15   transferring an encryption key across a communication link, according to an embodiment of the present invention.

Figure 5 is a flowchart illustrated the steps of a process of securely transferring an bitstream between logical circuits, according to an embodiment of

20   the present invention.

Figure 6 is a schematic of a computer system, which may be used to implement embodiments of the present invention.

Figure 7 is a schematic illustration of a local encryptor with multiple hidden registers and a control register, according to an embodiment of the present invention.

5   Figure 8 is an illustration of an exemplary digital bitstream decryptor and decoder with non-volatile memory, according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following detailed description of the present invention, a method and system for securely decrypting and decoding a digital signal, numerous specific details are set forth in order to provide a thorough understanding of the present

5   invention. However, it will be recognized by one skilled in the art that the present invention may be practiced without these specific details or with equivalents thereof. In other instances, well known methods, procedures, components, and circuits have not been described in detail as not to unnecessarily obscure aspects of the present invention.

10

NOTATION AND NOMENCLATURE

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits that can be performed on computer

15   memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer executed step, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring

20   physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in a computer system. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols,

25   characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise

5   as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as "indexing" or "processing" or "computing" or "translating" or "calculating" or "determining" or "scrolling" or "displaying" or "recognizing" or "generating" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that

10   manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

15   <u>METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER</u>

The present invention provides for a method and system for securely decrypting and decoding a digital signal. In order to combat theft of encryption keys on a communication link, embodiments of the present invention encrypt the key itself before transferring it across a bus. Additionally, embodiments also

20   provide for a local encryption key so that the bitstream is not exposed un-encrypted on the pins of an integrated circuit.

Figure 2 illustrates a diagram of an exemplary digital decoder 200. The decoder 200 comprises a first logical circuit 203 and a second logical circuit 204.

25   The logical circuits may be, for example, separate integrated circuits. Additionally,

SONY-50P4042 US P

the system comprises a hard disk drive 217, which may be used for storing (recording) digital signals. These signal may be transferred over the IEEE 1394 bus 216 in an encrypted form.

5   The first logical circuit 203 comprises a broadcast encryptor 202, a local encryptor 220, a Digital Transmission Content Protection (DTCP) block 223, and a switch 205 connecting local encryptor 220 to either the DTCP block 223 or the broadcast decryptor 202. The broadcast decryptor 202, local encryptor 220, and local decryptor 221 have hidden registers 310c, 310a, and 310b respectively.

10

The second logical circuit 204 comprises a local decryptor 221, a transport parser/de-multiplexer 207 which parses and de-multiplexes the decrypted bitstream. Additionally, this circuit 204 has a video decoder 208 and audio decoder 209. Finally, the circuit has interfaces such as Smartcard interface 210

15   and bus interfaces 206 and 211.

Bus interfaces 206 and 211 may be any of a variety of physical bus interfaces, including but not limited to a Universal Serial Bus (USB) interface, Personal Computer (PC) Card interface, CardBus or Peripheral Component

20   Interconnect (PCI) interface, mini-PCI interface, Personal Computer Memory Card International Association (PCMCIA) interface, Industry Standard Architecture (ISA) interface, or RS-232 interface.

The system also comprises a host computer system 214, which may be a

25   computer system such as illustrated in Figure 6. The host computer system 214 is

SONY-50P4042 US P

separate from the first 203 and second 204 circuits in that a communication link

215 or other mechanism separates them. For security, embodiments of the

present invention will encrypt keys transferred between the host computer 214 and

the circuits (203, 204). In a preferred embodiment, communication link 215 is a

5   PCI bus.

Referring now to Figure 3a, the local encryptor 220 will be discussed in

more detail. The local encryptor 220 inputs an un-encrypted bitstream 314 from

another part of the first logical circuit 203. The local encryptor 220 outputs an

10   encrypted bitstream 342, which may be input to the local decryptor 221. The local

encryptor 220 also may communicate with the host processor 214 via the

communication link 215. The local encryptor 220 comprises an even key register

302a and an odd key register 304a, which may be used for storing even and odd

encryption keys, respectively.

15

The hidden register 310a is used to store a value which, in one

embodiment, the host computer system 214 may access and use to encrypt keys

before transferring them across a communication link 215. After transfer, the same

value is used by the first circuit 203 to decrypt the key. The value may be stored in

20   the hidden register 310a when the circuit 203 is manufactured. The present

invention provides considerable flexibility regarding the hidden registers 310. In

one embodiment, a software engineer, who knows the value stored in the hidden

registers 310, provides this information to the host computer system 214. In this

fashion, the host system 214 does not need to access the hidden registers 310.

SONY-50P4042 US P

Thus, the connection between the hidden register 310a and the communication link 215 is optional.

5   In one embodiment, the hidden register 310a is non-volatile. In one embodiment, the host computer 214 may write to the hidden registers 310. In one embodiment, the hidden register 310a is 64 bits. However, the present invention is well-suited to hidden registers 310 of other sizes, as it may be useful, although it is not required, for the hidden register 310a to be the same size as the broadcast key.

10

The encryptor 220 also contains key decryption logic 312a, which uses the value in the hidden register 310a along with knowledge of the process used to encrypt the key to decrypt it. For example, if the key was encrypted by performing an exclusive OR with the key and the value from the hidden register 310a, then the

15   key decrypt logic 310a performs an exclusive OR on the encrypted key with the value from the hidden register 310a to obtain the original un-encrypted key. The present invention is well-suited to other methods of encrypting/decrypting the key while using the value from the hidden register 310a.

20   Still referring to Figure 3a, the local encryptor 220 also has bitstream encrypting logic 306. This logic 306 make use of the key passed to it from the host computer system 214. Finally, the local encryptor 220 has a Transport Scrambling Control (TSC) register 308. This register 308 may be written to by the host computer system 214 to direct the encryptor 220 to modify the TSC bits in the

25   header of the signal bitstream to indicate that the bitstream is encrypted and

whether the encryption is odd or even. For example, the transport scrambling control bits in the transport packet may be set to "10" for an even key and "11" for an odd key. The bits may also be set to "01" to indicate the bitstream is not scrambled. The present invention is not, however, limited to using the values with

5   the control register 308 in this fashion. The value in the TSC register 308 may also be used to determine which key register (302a, 304a) should be selected by encryptor switch 303.

Referring now to Figure 3b, the local decryptor 221 outputs a decrypted

10   bitstream 344 and contains logic similar to the local encryptor 220. For example, it contains an even key register 302b, an odd key register 304b, a hidden register 310b, and key decryption logic 312b. The local decryptor 221 also contains logic 326 suitable to decrypt the bitstream 342 which the local encryptor 220 encrypted. The bitstream decryptor 326 reads the TSC bits in the bitstream 342 and uses that

15   value to determine whether to use the even key or the odd key. For example, switch 325 may be controlled by TSC signal 328. The connection between the hidden register 310b and the communication link 215 is optional. The broadcast decryptor 202 features the same logical circuitry as the local decryptor 221.

20   Referring now to Figure 4, the steps of a process 400 for encrypting keys before transferring them across a bus (e.g., communication link 215) will be discussed. Process 400 may be implemented as instructions stored in computer memory and executed over a processor of any general purpose computer system. In step 405, an encrypted bitstream is received, for example, by frontend (Figure 2,

25   201).

In optional step 410, a hidden register 310 is accessed by the host computer system 214. In one embodiment, the developer of the software for host system 214 has knowledge of how to access the hidden register 310; however, the

5   hidden register 310 is otherwise inaccessible so as to minimize theft of the encryption keys and hence the encrypted signal. Conveniently, this hidden register 310c may be within the broadcast decryptor 202, as the key will be sent to that component. However, in other embodiments, the hidden register 310 may be anywhere in first circuit 203.

10

In one embodiment, the host computer system 214 has knowledge of the value in the hidden register 310; therefore, it does not need to access the hidden register 310. For example, a software engineer provides the host system 214 with the value which was or will be stored into the hidden register 310 at manufacture

15   time. In this embodiment, the hidden register 310 may be inaccessible from outside the circuit, thus providing added security.

In step 415 the broadcast key is determined at a location separate from where the bitstream is to be decrypted. For example, the key may need to be

20   transferred across a communication link 215 to get to the broadcast decryptor 202. To determine the key, key information may be extracted from the bitstream and sent the host computer system 214. The host system 214 communicates with the Smartcard 213 to determine the encryption key. The present invention is well-suited to using other methods for determining the broadcast encryption key. For

25   example, the Smartcard 213 is for illustrative purposes only. This key may be

frequently renewed and may be an odd or an even key, and may be accomplished using well known methods.

In step 420, the host computer system 214 encrypts the broadcast key. The value which is in the hidden register 310c in the first logical circuit 203 is used. Consequently, the first circuit 203 will be able to decrypt the broadcast key using this value, provided the first circuit 203 knows the encryption method used by the host computer system 214. As stated herein, the present invention, provides great flexibility regarding the hidden registers 310, which may be read or written, but do not have to be, in various embodiments.

In step 425, the encrypted broadcast key is transferred across the bus 215 by the host system 214. As the key is encrypted, the conventional art problem of theft is minimized dramatically.

In step 430, the first circuit 203 decrypts the broadcast key. The first circuit 203 has access to the value in the hidden register 310c, which it uses, along with knowledge of the encryption technique, to decrypt the key. For example, in one embodiment an exclusive OR is performed between the value in the hidden register 310c and the encrypted key.

Using this key, the first circuit 203 is now able to decrypt the signal (bitstream), in step 435. The signal may now be sent to the DTCP block 223 so that the signal may be encrypted for transfer across to IEEE 1394 bus and stored

for later play. Alternatively, the signal may be sent directly to the local encryptor 220 such that the signal may be transferred to the second logical circuit 204.

Referring now to Figure 5, the steps of a process 500 for securely 5 transferring a bitstream between circuits will be discussed. Process 500 may be implemented as instructions stored in computer memory and executed over a processor of any general purpose computer system. In step 505, the local encryptor 220 receives the un-encrypted signal from either the broadcast decryptor 202 or the DTCP decryptor 233.

10

In optional step 510, the hidden registers 310a and 310b are accessed by the host computer system 214. Other embodiments provide the host system 214 with the value in the hidden registers 310 in other fashions, as described herein. In one embodiment, the hidden registers 310a and 310b, respectively, in circuits 15 220 and 221 contain different values. Furthermore, even if the values from one set-top decoder box are discovered, the security of other boxes in not compromised, because other boxes are manufactured with different values.

In step 515, the local encryption key (odd or even) is generated by the host 20 computer 214. The process 500 cycles from step 515 through step 560 with the host processor 214 alternating between sending out odd and even keys. Additionally, the local encryption key generated in one set-top box system may be different from other set-top boxes. Therefore, even were the local encryption key to be stolen, it would do no good to pass it to another set-top box. This is in

contrast to some conventional systems for which all set-top boxes use the same encryption key, at least for a period of time.

5   In step 520, the local key is encrypted for the first 203 and the second 204 circuits. In a preferred embodiment, an Exclusive OR is performed between the value from a hidden register 310 and the local key. Because the first and second circuits may have their own hidden register 310 values, the encryption will be different for each circuit.

10   In step 525, the encrypted keys are transferred across the bus 215 to the first 203 and the second 204 circuits. A 64-bit value in the hidden register 310 will provide 2^{64} possible combinations. Therefore, it will be very difficult to obtain the original key from the encrypted (XORed) key without the secret hidden value.

15   In step 530, the host computer 214 sends a command to the first circuit 203 to modify the TSC bits in the header of the bitstream to indicate that the bitstream is encrypted. Additionally, the command may indicate the type of encryption key, for example, odd or even. The circuit 203 then modifies the header to indicate the type of encryption key.

20

           In step 535, the local key is decrypted at the first circuit 203 using the value from the hidden register 310a. In step 540, the second encrypted local key is decrypted at the second logical circuit 204. The odd and even key registers (304b, 302b) allow the host computer 214 to send the ever changing keys out somewhat

25   ahead of the time the bitstream requires a new key for decryption.

Then, in step 545, the bitstream is encrypted, for example by bitstream

encryption logic 306. Any convenient encryption method may be used here, for

example, data encryption standard (DES) may be used.

5

In step 550, the TSC bits are modified in the bitstream header. In this

fashion, the local decryptor 221 will be able to determine necessary information to

decrypt the locally encrypted bitstream 342, for example, whether the key is odd or

even. This facilitates key switching which makes theft of the bitstream more

10   difficult.

In step 555, the bitstream is transferred from the first integrated circuit 203 to

the second integrated circuit 204. Unlike some conventional systems, the

bitstream is encrypted for protection, in this embodiment.

15

In step 560, the local decryptor 221 uses the local encryption key to decrypt

the signal it received from the local encryptor 220. In step 565, the decrypted

bitstream 344 is sent on to the transport parser/de-multiplexer 207 and so on for

decoding.

20

For added security, an embodiment illustrated in Figure 7 contains multiple

hidden registers. While the local encryptor 220 is shown, this embodiment is

equally suited to the decryptors (202, 221). At least one hidden register 310 is

selected for use, for example, by the host computer system 214. The selected

25   hidden register(s) 310 may be indicated to the first and second circuits (203, 204)

via a bit or bits which are set in a control register 315. For example, in one embodiment, the host processor 214 may use the value in either a first hidden register 310 or a second hidden register 310 or both hidden registers 310 in the encryption process. Any suitable method may be used to indicate which hidden

5 register(s) 310 are used. For example, a value of "01" for a first hidden register, "10" for a second hidden register, and "11" for both is sent from the host 214 to the control register 315. The present invention is well-suited to using any number of hidden registers 310. Furthermore, the host 214 may periodically change the value in the control register 315 (along with the key encryption).

10

Referring to Figure 8, in yet another embodiment, rather then using a hidden register 310, user-dependent data may be used to derive local encryption keys. For example, the digital bitstream decryptor and decoder 200 has non-volatile memory 317 to store user-dependent data, such as favorite TV programs,

15 pay-per-view charges, etc. The host computer system 214 accesses this non-volatile memory 317 to generate a unique key for each set-top box (e.g., digital bitstream decryptor and decoder 200).

For still more secure key encryption other bit operations such as bit-

20 inversion, bit-shift, bit-permutation, or the like may be applied. In one embodiment, these operations are combined. Furthermore, the combinations used may be varied. In these embodiments, the host processor 214 will indicate to the circuits (203, 204) which encryption method is currently being used.

Another embodiment provides for a method of detecting possible tampering with the system. In this method, the host computer 214 periodically polls all the related hidden registers 310 in broadcast decryptor 202, local encryptor 220, and local decryptor 221. If a discrepancy is detected, host computer system 214 goes

5   into emergency mode and shuts down the whole system. Furthermore, host computer system 214 may send out an alert to the broadcast service provider indicating the possible tampering. This embodiment, makes it difficult for a hacker to illegally modify the values in the hidden registers 310.

10   Figure 6 illustrates circuitry of computer system 100, which may form a platform for a portion of the host computer system 214, the broadcast decryptor 203, the local encryptor 220, or the local decryptor 221. Computer system 100 includes an address/data bus 99 for communicating information, a central processor 101 coupled with the bus for processing information and instructions, a

15   volatile memory 102 (e.g., random access memory RAM) coupled with the bus 99 for storing information and instructions for the central processor 101 and a non-volatile memory 103 (e.g., read only memory ROM) coupled with the bus 99 for storing static information and instructions for the processor 101. Computer system 100 also includes an optional data storage device 104 coupled with the bus 99 for

20   storing information and instructions.

Also included in computer system 100 of Figure 6 is an optional alphanumeric input device 106. Device 106 can communicate information and command selections to the central processor 101. System 100 also includes an

25   optional cursor control or directing device 107 coupled to the bus 99 for

communicating user input information and command selections to the central

processor 101. The display device 105 utilized with the computer system 100 may

be a liquid crystal device, cathode ray tube (CRT), field emission device (FED, also

called flat panel CRT) or other display device suitable for creating graphic images

5   and alphanumeric characters recognizable to the user. Signal input/output

communication device 108 is also coupled to bus 99.

The preferred embodiment of the present invention a method and system

for securely decrypting and decoding a digital signal is thus described. While the

10   present invention has been described in particular embodiments, it should be

appreciated that the present invention should not be construed as limited by such

embodiments, but rather construed according to the below claims.